Vol.2021-CSEC-93 No.8
Vol.2021-IOT-53 No.8
2021/5/13

重要度を考慮した脆弱性評価システム

山越 大雅[1]　田島 浩一[2]　近堂 徹[2]　渡邉 英伸[2]　岸場 清悟[2]　西村 浩二[2]　相原 玲二[2]

概要：脆弱性診断は，Web コンテンツ，コンピュータ，ネットワーク等に対して擬似攻撃を行い，内部に潜む脆弱性を発見する診断であり，昨今のサイバー攻撃の脅威に備えるために世界中のあらゆる組織で必要不可欠なものとなっている．一般的に，診断結果には脆弱性が危険度によりレベル分けされており，それがそのまま対策の優先度として利用されているという問題点が指摘されている．この問題に対して本研究では，セキュリティインシデントにつながる可能性を元に対策の優先度を評価し，反映した診断結果を提供する脆弱性評価システムを開発した．脆弱性評価システムでは，脆弱性診断により得られる診断結果を対象とし，診断結果に含まれる CVE（脆弱性の識別子）などの識別子や脆弱性情報として公開されている NVD および JVN のデータベース等を用いて評価を行う．また，広島大学で実施している脆弱性診断の診断結果を処理対象として例を示す．

Development of a vulnerability assessment system considering the importance

Abstract: Vulnerability assessment is attacking to Web contents, computer, network, and so on to find vulnerability, and it’s necessary for many organizations. In general, the risk of vulnerabilities is separated to some levels, but it’s used for urgency to solution. In this paper, we developed “Vulnerability Assessment System” to assess urgency for solution from vulnerabilities can lead to security incidents. Vulnerability Assessment System assesses vulnerabilities by using CVE and Database such as NVD and JVN. Moreover, we present some examples using the diagnosis that assessed in Hiroshima University.

1. はじめに

大学などの高等教育機関において，キャンパスネットワークには一般的なサーバや実験装置・機器等が多数接続される．これらの機器がインターネットからアクセス可能な場合，外部からの不正侵入アクセスによる情報漏洩・データ改ざん等のセキュリティインシデントにつながる脆弱性に細心の注意を払う必要がある．一方で，機器を所有する学内構成員が適切な管理・運用を行うことが望ましいが，その対応にはばらつきが生じる．その結果，安全性を維持するために多くの時間的コストと知識が必要となる．このような問題から定期的な脆弱性診断が効率的なセキュリティ対策として必要となる．脆弱性診断では，脆弱性診断ツールがよく用いられる．ツールによる診断は，プログラムによってコンテンツ，OS・ミドルウェア，ネットワークなどの既知の脆弱性を網羅的に検査するものであり，自動で脆弱性のリスクを評価し，診断結果までを一つのレポートとしてまとめてくれる．組織内にある数百台規模のサーバに対して定期的に脆弱性診断を行う場合，脆弱性診断ツールの結果をもとに各サーバ管理者が素早く対策を講じることで，コストを抑えつつサーバのセキュリティを最新の状態を保ち，未然に攻撃を防ぐことが期待される．ツールによる診断は機械的な検査であるため，過検知・誤検知などが含まれる場合があるものの，サーバ管理者が自身の管理状況をもとにその情報を見直すことで的確な情報を得られることもあり，手軽さとコストの観点から多くの組織で利用されている．一方，コンテンツ管理者，ホスト管理者，ネットワーク管理者など複数の管理者がいる場合においては，サーバに潜む脆弱性が一つにまとめられたレポートから，誰がどの脆弱性を対応すべきか管理者側で取捨選択することが要求される．また，深刻な脆弱性以外に，開発の終了に伴うリスクを指摘する警告等も含まれるた

[1] 広島大学　先進理工系科学研究科　理工学融合プログラム
Transdisciplinary Science and Engineering Program, Advanced Science and Engineering, Hiroshima University
[2] 広島大学　情報メディア教育研究センター
Information Media Center, Hiroshima University

め，情報量が膨大なものとなり，ひとつひとつ分析し対策を実施することは各管理者にとって非常に負担が大きい．そのため，多くの管理者は，単純に脆弱性診断結果のリスクが高いものを優先して対応しているのが現状となっているが，この方法では，管理体制や管理状況を考慮した的確な情報になっていない可能性があることから，本来優先して対策すべき脆弱性への対応が後回しにされる可能性があることが指摘されている．

このような背景から，本研究では重要度を考慮して脆弱性の評価を行うシステムの開発を行った．本稿では，脆弱性評価システムがどのようにしてそれらの問題点を解決するのかを述べ，評価を行う．また，脆弱性評価システムの試作を通じて得られた知見をもとに，今後の脆弱性評価システムの展望について示す．

2. 現状の脆弱性診断における課題と要件

広島大学，鹿児島大学，信州大学では，脆弱性診断ツールとして Nessus を用いた脆弱性診断が行われている [1–4]．Nessus は商用の脆弱性診断ツールであり，過検知や誤検知が比較的少なく，過去に多くのゼロデイの脆弱性を早急に発見した実績もあることから，診断能力の高い脆弱性診断ツールとして世界中で利用されている．Nessus を含む多くの脆弱性診断ツールのレポートは，検知された脆弱性毎に危険度が示されている．危険度は低い順に Low, Medium, High, Critical となっており，Common Vulnerabilities Scoring System（CVSS）[5,6] で算出されたスコア値に基づいて危険度が自動で決定される．

既存の脆弱性診断における評価方法にはいくつかの課題が存在する．一つ目は，対策を行う際の優先度が CVSS をもとに判断されている点である．Jonathan M. Spring らの提供する Stakeholder-Specific Vulnerability Categorization（SSVC）[7] では，CVSS の評価を対策の優先度として利用すると，本来優先して対策すべき脆弱性が後回しにされてしまうことが指摘されている．二つ目は，管理者が優先的に防ぎたい攻撃や各管理者の役割を考慮した対策の重要度が危険度の評価に含まれていない点である．一般的な組織における管理者階層を図 1 に，また各管理者における役割と優先的に防ぎたい影響の関連性を表 1 に示す．なお，3 つの管理者の立場と役割については，3.2 節で詳説する．脆弱性の危険度の評価に影響を受ける管理者を考慮していない場合，適切な評価が行われず，対策が行われないことや後回しになることがある．

適切な評価のための解決策の一つとして，SSVC が提案されている．SSVC は管理者の役割毎に脆弱性の影響を受けるすべての要素と各影響の大きさの関係を決定木上に構築し，すべての要素に対応すべき優先度を 4 段階で決定していく方法である．一方，複数の管理者がいた場合，それぞれ決定木が異なるため，同じ脆弱性に対して優先度が異なる状況が生じてしまい，管理者間で優先度の再調整が必要となる．また，決定木の作成はサーバの管理状況を把握している管理者側に求められ，決定木の要素を追加・削除する場合においても，結局決定木全体を見直す必要があり，実用面で改善の余地が残る．

現状の脆弱性診断の課題を解決するためには，管理者の役割と対策ポリシーを考慮した危険度の評価と対策の優先度を機械的に評価することが重要である．影響を受ける管理者を判定し，危険度の評価と対策の優先度を自動で評価することで影響を受ける管理者にとって優先的に防ぎたい攻撃を考慮した適切なセキュリティ対策が可能となる．

3. 脆弱性評価システム

3.1 脆弱性評価システムの構成と 2 つの評価機能

脆弱性評価システムは，管理者の役割や対策ポリシーを考慮し，危険度と対策の優先度を機械的に評価することを目的に開発した．脆弱性評価システムの構成を図 2 に示す．Nessus 等の脆弱性診断のレポートを入力として，以下に示す 2 つの機能を実施したのちに，重要度に応じた脆弱性評価結果を出力する．

機能①

機能①は，影響を受ける管理者と対策を行う管理者の判定である．例えば，脆弱性診断の結果，PHP に脆弱性が存在する場合は，影響のある管理者はコンテンツ管理者と判定される．また，対策を行う管理者はホスト管理者と判定され，アップデートを行う．

機能②

機能②は，脆弱性の危険度と対策の優先度を評価する機能である．脆弱性の危険度は，情報セキュリティの 3 要素を利用して評価する．情報セキュリティの 3 要素は，情報漏洩の可能性を評価する「機密性への影響」，情報が改ざんされる可能性を評価する「完全性への影響」，サービスの遅延・停止の可能性を評価する「可用性への影響」である．機能①より得られる影響を受ける管理者によって重視する評価のそれぞれの要素が変化するように設計した．例えば，コンテンツ管理者はサービスの停止を優先的に防ぎたいという考えのもと

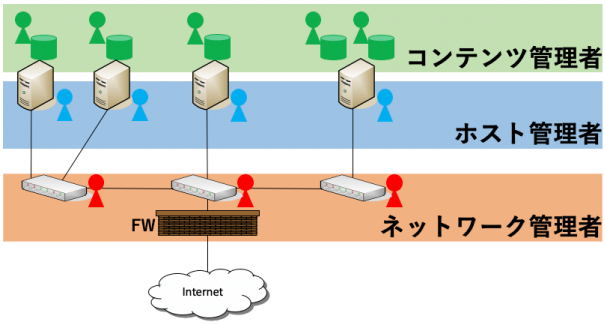

図 1 各管理者の関係図

表 1　各管理者の役割と対策ポリシー

管理者	役割	対策ポリシー（優先的に防ぎたい影響）
ネットワーク管理者	ネットワーク機器の運用・設定・保守	ネットワーク機器の停止
ホスト管理者	各種サーバ管理	重要情報の漏洩・改ざん
コンテンツ管理者	Web サイトの運営・保守	サービス停止

「可用性への影響」を重視した評価手法となっている．対策の優先度は，攻撃元区分や攻撃条件の複雑さを利用して評価する．これは，対策を行う優先度を脆弱性の危険度で評価するのではなく，管理者にとってどれだけ防ぎたいものなのかということや，攻撃者がどれだけ攻撃しやすいのかなどを考慮して評価する．これによって迅速な対策と利用者の対策ポリシーと環境を考慮した評価が可能になると考えている．また，脆弱性の種類を識別する際に用いる CWE を利用して危険度の評価を調整する．CWE は毎年危険な CWE 上位 25 位 [8] を発表している．これを用いることで脆弱性の流行を取り入れ，どの脆弱性が特に危険なのかを評価することができる．

3.2　組織の管理階層

本研究が想定する組織の管理階層について説明する．管理者はネットワーク管理者，ホスト管理者，コンテンツ管理者が存在することを想定している．それぞれの基本的な役割は一般の組織や広島大学では同じである．一般的にネットワーク管理者はネットワーク機器に関する業務やネットワーク環境における設定や保守を行う．ホスト管理者は，サーバの管理やサーバにアクセスするホストの監視などを行う．コンテンツ管理者は，Web サイトの運営や保守などである．表 1 は各管理者が組織においてどのような役割があるのかを表している．組織によって管理者に与えられている権限や管理範囲は異なっているため，脆弱性評価システムでは，利用対象を考慮した評価を行うように設計した．

3.3　脆弱性の評価手法

3.3.1　影響を受ける管理者の判定

影響を受ける管理者の判定は，危険度と対策の優先度を調整する際に必要となり， 脆弱性診断によって得られるレポートに記載されている概要の項目を用いて行う. 処理方法としてはキーワード判定をプログラム処理で行う．例えば，2019 年に公開された Web サーバソフトの Apache に関する脆弱性 CVE-2019-0196 [9] では，概要は「Apache 2.4.x<2.4.39 Multiple Vulnerabilities」となっている．この脆弱性によって攻撃対象はサービス運用妨害状態にされる可能性がある．この場合に影響を受ける管理者は「コンテンツ管理者」としている．また，プログラム処理で「Apache」がキーワード判定されるように設計している．

3.3.2　対策を行う管理者の判定

対策を行う管理者の判定は，影響を受ける管理者と同様に危険度と優先度の評価の際に必要となり，レポートに記載されている対策方法を用いて行う．判定される対策の種類については，ソフトのアップデートや特定のホストからのアクセス遮断，プログラムや設定の修正，ソフトの開発元などに確認する大きく分けて 4 つの対策に分けられる．処理方法は，影響を受ける管理者の判定と同様にキーワード判定を行う．例えば，CVE-2019-0196 の脆弱性の対策は「Upgrade to Apache version 2.4.39 or later」となっており，アプリケーションのアップデートが必要であることがわかる．ここからキーワードとして「Upgrade」,「Apache」の 2 つを設定し，ホスト管理者が対策を行い，対策はアップデートとする．

3.3.3　危険度の評価

危険度の判定は，CVSS の評価値が算出される際に利用される要素を用いて脆弱性の独自の危険度と対策の優先度を評価する．評価の際に利用する要素の抽出は，CVE を用いて図 2 のように MyJVN API [10] と Vuls [11] のデータベースを活用する．危険度の評価は，CVSS の評価値算出の要素のうち，表 2 のものを利用する．CVSS の各要素は，CVE を用いて Vuls のデータベースより取得する．CVE が 2015 年以前のものは，CVSS がバージョン 2 のものしかないためそれを利用し，2015 年以降のものは CVSS がバージョン 3 のものを利用する ．

危険度の評価は，機密性への影響，完全性への影響，可用性への影響のスコアを下の数式で合計値を算出する．まずは，算出された値によって危険度をレベル分けする．表 3 は値によってどのように評価が変わるのかを示しており，これは CVSS の算出を参考にしている．例えば，機密性への影響が「全面的」でその他は「なし」の場合，以下の算出式（1）で計算を行うと合計値は 0.56 となり，表 3 より危険度は MIDDLE となる．危険度の評価の閾値は，機密性への影響，完全性への影響，可用性への影響の評価を考慮して作成した．評価が「NONE」の場合は，3 つの評価が全て「なし」のときである．評価に 1 つ「部分的」が存在する場合は，評価は「MIDDLE」となり，「部分的」が 2 つと「なし」以外の評価がある場合，評価が「HIGH」となる．また，脆弱性の CWE が CWE TOP 25 に該当する場合は，危険度が 1 段階上がるように設計しているため，危険度が「HIGH」と評価され CWE が CWE TOP 25 に該当する場合は，「CRITICAL」へと変化する．

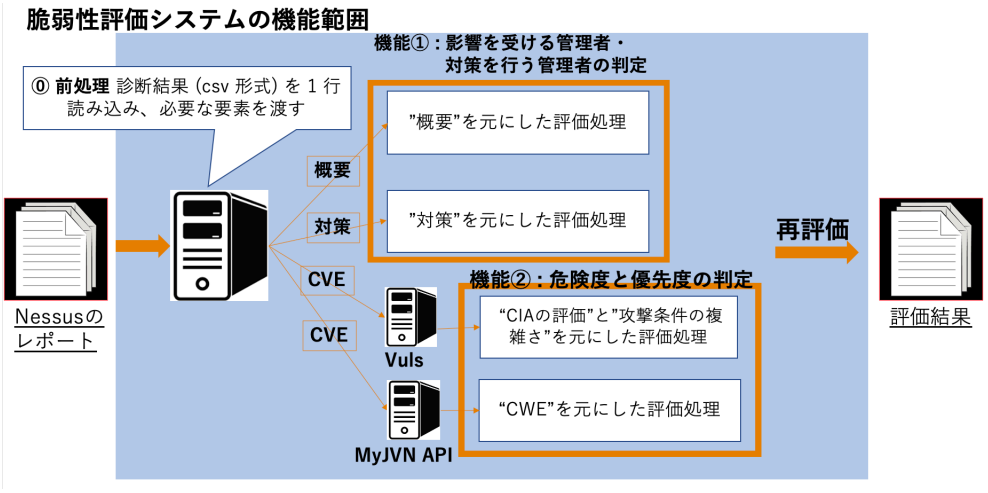

図 2 脆弱性評価システムの構成

表 2 CVSS の要素（抜粋）

CVSS の要素	概要	評価レベル（スコア）
機密性への影響	情報が漏洩する可能性を評価	なし（0）/部分的（0.22）/全面的（0.56）
完全性への影響	情報が改ざんされる可能性を評価	なし（0）/部分的（0.22）/全面的（0.56）
可用性への影響	サービスが遅延・停止する可能性を評価	なし（0）/部分的（0.22）/全面的（0.56）
攻撃元区分	どこから攻撃対象に攻撃可能かを評価	ローカル/隣接/ネットワーク
攻撃条件の複雑さ	攻撃の際に必要な攻撃条件の複雑さを評価	高/中/低

機能①によって得られる影響を受ける管理者の判定も危険度の評価の際に取り入れている．ネットワーク管理者とホスト管理者は多くの重要な情報を管理していることから情報の漏洩や改ざんといった「機密性への影響」と「完全性への影響」のある攻撃を優先的に防ぎたいと考えており，コンテンツ管理者は，Web サービスの停止といった「可用性への影響」のある攻撃を優先的に防ぎたいと考えている．これらは，重視する要素に影響がある場合は，危険度が 1 段階上がるように設計した．例えば，コンテンツ管理者に影響のある脆弱性で「可用性への影響」が該当し，Nessus による診断結果が Low の場合は，MIDDLE へと上がるようにしている．

脆弱性の危険度がどのように評価されるのか，CVE-2019-0196 を例に，図 3 で説明する．この脆弱性は「可用性への影響」のみが LOW と評価され，それ以外は NONE となっている．このことからまず，危険度は LOW と評価される．次に，影響を受ける管理者がコンテンツ管理者でありサービス停止といったような影響のある攻撃を優先的に防ぎたいため危険度を 1 段階上げ MIDDLE とする．さ

表 3 合計値と評価

合計値	評価レベル
0	NONE
0.230	LOW
0.570	MIDDLE
0.915	HIGH
0.915 + α	CRITICAL

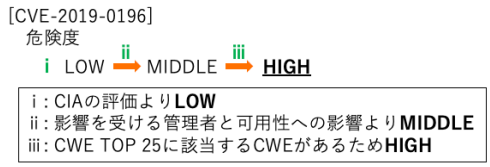

図 3 危険度の評価の変化

らに，この脆弱性に含まれる CWE が CWE TOP 25 に該当するためもう 1 段階危険度を上げ HIGH となる．脆弱性評価システムの出力において，危険度は数値で出力される．Nessus では，Medium などと出力されるが，脆弱性評価システムでは，NONE は 0，LOW は 1，MIDDLE は 2，HIGH は 3，CRITICAL は 4 として出力される．

$$(\text{合計値}) = 1 - \{(1 - [\text{機密性への影響}]) \times (1 - [\text{完全性への影響}]) \times (1 - [\text{可用性への影響}])\} \quad (1)$$

3.3.4 優先度の評価

優先度の基本評価は表 4 のようになっている．これは，危険度と優先度が同様の評価となるようにしているが，危険度の評価が MIDDLE と HIGH の場合には，異なるものにしている．広島大学で行われた脆弱性診断の結果より，危険度の評価が High のものが多く存在していたが，緊急に対策が必要なものが多くなかったため危険度が HIGH の場合には優先度は MIDDLE としている．対策の優先度は，攻撃元区分や攻撃条件の複雑さによって評価を変える．

図 4 優先度の評価の変化

攻撃元区分が「ネットワーク」かつ，攻撃条件の複雑さが「低」の場合，優先度の評価を 1 段階上げるように設計している．危険度の評価で用いた例では，危険度は MIDDLE と評価され，基本の優先度の評価は MIDDLE となる．しかし，攻撃元区分が「ネットワーク」で攻撃条件の複雑さが「低」の場合は，1 段階上げられ「HIGH」という評価となる．

対策の優先度がどのように評価されるのかを図 4 で説明する．まず，危険度が HIGH と評価されたことから優先度は，MIDDLE と評価される．（表 4）しかし，この脆弱性の攻撃元区分は「ネットワーク」となっており，遠隔から攻撃することが可能となっている．また，攻撃条件の複雑さが「低」となり，攻撃がしやすくなっている．どちらの評価要素も最も危険度が高くなっていることから優先度を 1 段階上げ，HIGH となる．対策の優先度の出力は危険度と同様の出力方法で数値が出力される．

3.3.5 評価処理の全体の流れ

4 つの評価処理がどのような過程で行われるのかを説明する．

STEP 0
: まずは，レポートに記載されている概要・対策・CVE 等の項目をプログラム処理によって抽出する．

STEP 1
: 概要を用いて影響を受ける管理者を判定する．また，対策を用いて対策を行う管理者の判定を行う．

STEP 2
: 脆弱性の危険度を評価するために機密性への影響，完全性への影響，可用性への影響が必要となる．STEP 0 で取得した CVE を用いて Vuls のデータベースよりそれら 3 つを取得する．それぞれの要素を数値化し，算出式（1）と表 3 を用いて危険度を求める．

STEP 3
: STEP 3 では，STEP 2 で求めた評価を用いて危険度の調整を行う．STEP 1 で判定した影響を受ける管理者を用いて，危険度を 1 段階上げるか判定する．ここで危険度が確定する．

STEP 4
: STEP 3 で評価された危険度を用いて，対策の優先度を評価する．優先度は表 4 より危険度によって決まる．そして，攻撃元区分と攻撃条件の複雑さをもとに調整を行う．それらの要素は，STEP 0 で取得した CVE を用いて Vuls のデータベースより取得する．攻撃元区分がネットワークで攻撃条件の複雑さが低の場合は，優先度が 1 段階上がる．

STEP 5
: CVE を用いて，MyJVN API を利用し CWE を取得する．取得した CWE が CWE TOP 25 に該当する場合には，より危険な脆弱性であると判断し，優先度が 1 段階上がる．ここで優先度が確定する．

表 4 優先度の基本評価

危険度の評価	優先度の評価
NONE	NONE
LOW	LOW
MIDDLE	MIDDLE
HIGH	MIDDLE *1
CRITICAL	HIGH

*1 危険度が HIGH の場合は優先度が MIDDLE である．

3.4 脆弱性評価システムの出力

Nessus には，HTML 形式のレポートとは別に CSV 形式のデータとして結果を出力する機能がある．脆弱性評価システムでは，対策を行う管理者別に評価結果のファイルを作成する機能を用意した．評価結果のファイルには，脆弱性のタイトルおよび判定結果を重要度順のリストとして提示し，対策や詳細情報は別に生成済みの HTML 形式のレポートへのリンクを用意し参照する構成とした．出力される評価結果には，HTML 形式の脆弱性の詳細へのリンクが記載されている．プログラム処理によって出力される脆弱性対策情報に全て情報を載せることはプログラム処理に時間がかかることや利用者にとって見にくいなどの問題点がある．そのため出力される診断結果には要点のみを載せ，詳細を知るためのリンクを追加で載せている．

脆弱性評価システムによって作成された評価結果は，対策を行う管理者がネットワーク管理者のみでない限りホスト管理者へ一括して通知される．そして，ホスト管理者は各管理者別に診断結果が作成されているためそのまま対象の管理者へ通知を行う．そのため，受け取った診断結果の分析が不要となる．

4. 評価

本節では，開発を行った脆弱性評価システムの評価と 2020 年 10 月に広島大学で行われた Nessus による診断結果レポートと比較を行う．

4.1 診断結果と評価結果の比較

結果が変化したものの例として，今回，17183 件の脆弱性があった中で CVE-2019-0196 を用いる．この脆弱性は，「Apache」の特定のバージョンに脆弱性が存在し，サービス運用妨害が引き起こる可能性がある．レポート（図 5）では危険度は 5 段階中，3 段階目の Medium と評価されて

おり，脆弱性評価システムによる評価結果（図 6）では危険度は 5 段階（0〜4）中，4 段階目（3）の HIGH と評価されている．さらに，優先度は同様に HIGH と評価され，影響を受ける管理者はコンテンツ管理者，対策を行う管理者はホスト管理者となっている．対策内容がソフトウェアのアップデートということから対策の種類はアップデートとなっている．影響を受ける管理者がコンテンツ管理者であり，サービス停止の可能性を評価する「可用性への影響」が該当していることや CWE TOP 25 に該当する CWE が含まれることから危険度は HIGH が妥当であると考えている．このように優先度と対策を行う管理者が記載されていることで診断結果を受け取った管理者は，診断結果の分析が必要ないため管理者への脆弱性情報の通知が容易に行うことができる．

4.2 危険度の評価の比較

Nessus によるレポートでの危険度別の警告数と脆弱性評価システムを用いた場合の危険度別の警告数を比較し，どのような変化をしたのかを説明する．危険度別の変化は図 7 のようになっている．脆弱性評価システムでは，評価は「Low」と「High」のものは半分以下になり，「Middle」が約 1.5，Critical が約 2 倍に増加した．これは，Nessus の診断結果では危険でないと評価されたものが役割やポリシーを考慮した場合，危険なものとして評価されたことを意味する．なお，脆弱性の評価の際に利用する機密性への影響が最も高い「HIGH」の場合，不正アクセスにより情報資産に流出が起こり，組織内への影響が考えられる．攻撃元区分が「ネットワーク」である場合は，遠隔からの攻撃が可能であるため攻撃の可能性が高くなる．攻撃条件の複雑さが「低」の場合は，攻撃が容易であることを意味する．その他には攻撃元区分や攻撃条件の複雑さ，含まれる CWE が危険なものである場合は危険度が上がる評価手法となっている．このように役割やポリシーを考慮し，機械的に危険度や対策すべき優先度を決定することで，複数の管理者間で優先度の再調整作業を不要としつつ，速やかな対応への誘導ができると考えている．

5. 脆弱性評価システムの利点と改善点

5.1 脆弱性評価システムの利点

脆弱性評価システムでは，脆弱性診断によって得られるレポートを用いて再評価を行った．それにより，Nessus による脆弱性診断とは異なる危険度の評価が出力されることがある．Nessus による脆弱性診断のレポートから検出される脆弱性の数が減るということではなく，危険度の評価が変わるだけである．脆弱性評価システムは利用者の役割と対策ポリシーを考慮した評価が行われることで効率的なセキュリティ対策を行うことが可能となる．脆弱性評価システムでは，Nessus による脆弱性診断とは異なり対策の優先度が出力される．これにより評価結果を受け取った管理者は優先度の高い順に脆弱性が並んでいるため効率的に対策を行うことが可能となる．

5.2 脆弱性評価システムの改善点

2020 年 4 月の広島大学で実施した脆弱性診断レポートを用いて脆弱性評価システムが適切に処理されるかを調査した．その結果，診断結果の全体の約 10%が新しい脆弱性で影響を受ける管理者と対策を受ける管理者の判定が不可能で，その他についても CVSS の各要素が取得できないものが存在した．そのため，英文においてキーワード判定を行うには，脆弱性の種類を把握し，各種類に該当する脆弱性のキーワードを網羅する必要がある．しかし，人の手でそれを行うことは非効率的であるため，何か他の方法で判定する方法が必要となる．また，そのためには脆弱性評価システムのシステム管理者という立場を設け，日々更新することで新しい脆弱性に対しても対応が可能となる．新しい脆弱性の危険度や優先度については，より適切な評価を行うために影響を受ける管理者の判定の精度を向上させ，各管理者が優先的に防ぎたい攻撃をランク付け等分析し，機密性への影響，完全生への影響，可用性への影響に異なる重みを付ける必要があるのではないかと考えている．また，脆弱性評価システムでは，システム開発の段階で管理者の優先的に防ぎたい攻撃が決められている．脆弱性評価システムを利用する組織では，決められた対策ポリシーとは異なる場合が存在する．そのため診断が実施される前に，管理者が優先的に防ぎたい攻撃などの情報を指定し，それに応じた危険度や優先度が算出されるようにすることで正確な評価を行い，適切なセキュリティ対策が可能となる．

6. おわりに

本論文では，既存の脆弱性診断における問題点を改善するために，セキュリティインシデントにつながる可能性を元に対策の重要度を評価し，反映した診断結果を提供する脆弱性評価システムの開発を行った．システムでは，対策を行う管理者の判定や脆弱性の危険性を利用者の対策ポリシーや環境を考慮した評価を行うことで，対策を行うべき管理者に対して重要度を考慮した脆弱性診断結果を提示することが可能となる．これにより，対策を行う前に脆弱性診断結果を受け取る管理者が行っていた診断結果の分析などの負担が軽減される．さらに，影響を受ける管理者を考慮して危険度や優先度を評価しているため，各管理者にとって適切な脆弱性の評価を提供でき，効率的な情報セキュリティ対策が可能となる．

Plugin ID	CVE	CVSS	Risk	Host	Protocol	Port	Name	Synopsis
84923	CVE-2019-0196	5.5	Medium	HOST A	tcp	80	Apache 2.4.x < 2.4.39 Multiple	The remote v

Description	Solution	See Also	Plugin Outpu	STIG Severit	CVSS v3.0 Ba
According to	Upgrade to Apache version 2.4.3	http://www.r	Source	: Server: Apa	7.8

図 5 Nessus の CSV 形式のデータ出力（抜粋）

Plugin ID	CVE	Host	Name	Solution
84923	CVE-2019-0196	HOST A	Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	Upgrade to Apache version 2

Risk(Nessus)	CWE	Risk	Urgency	Affected Admin	Admin taking action	Link
Medium	CWE-416	3	3	CONTENT Administrator	HOST Administrator (Update	Zone-A-

図 6 脆弱性評価システムによる評価結果

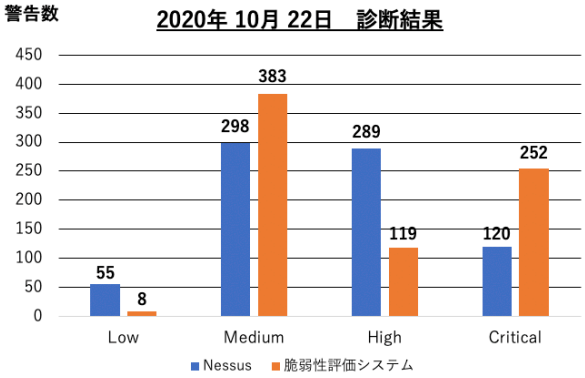

図 7 危険度別の警告数

参考文献

[1] 田島浩一, 岸場清悟, 大東俊博, 岩田則和, 西村浩二, 相原玲二, 広島大学におけるセキュリティ脆弱性診断の実施とその評価 学術情報処理研究, No.18 2014, pp.16-23
[2] 相羽俊生, 川原智徳, 高橋至, 小田謙太郎, 古屋保, 下園幸一, 佐藤豊彦, 升屋正人, 森邦彦, 学内サーバの脆弱性診断と診断結果の解析方法, 学術情報処理研究 No.20 2016, pp.105-111
[3] 浅川圭史, 中村文, 永井一弥, 今井美香, 伊藤稔, 長田和宏, 小幡美紀, 鈴木彦文. 不破泰, 学内サーバ管理の問題点と新たなサーバ管理方式について, 学術情報処理研究, No.18 2014, pp.1-8
[4] The Nessus Family https://www.tenable.com/products/nessus（最終アクセス日 2021-4-7）
[5] 共通脆弱性評価システム CVSS 概説 https://www.ipa.go.jp/security/vuln/CVSS.html（最終アクセス日 2021-4-1）
[6] 共通脆弱性評価システム CVSS v3 概説 https://www.ipa.go.jp/security/vuln/CVSSv3.html（最終アクセス日 2021-4-1）
[7] Jonathan Spring, Eric Hatleback, Allen D. Householder, Art Manion, Deana ShickPrioritizing, "Vulnerability Response: A Stakeholder-Specific Vulnerability" CategorizationCarnegie Mellon University
[8] 2020 CWE Top 25 Most Dangerous Software Weaknesses https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html（最終アクセス日 2021-4-1）
[9] CVE-2019-0196 https://nvd.nist.gov/vuln/detail/CVE-2019-0196（最終アクセス日 2021-4-4）
[10] MyJVN API とは https://jvndb.jvn.jp/apis/（最終アクセス日 2021-4-1）
[11] Vuls, https://vuls.io（最終アクセス日 2021-4-1）